2.ESTRUCTURA GENERAL

2.1.Esquema estructural.

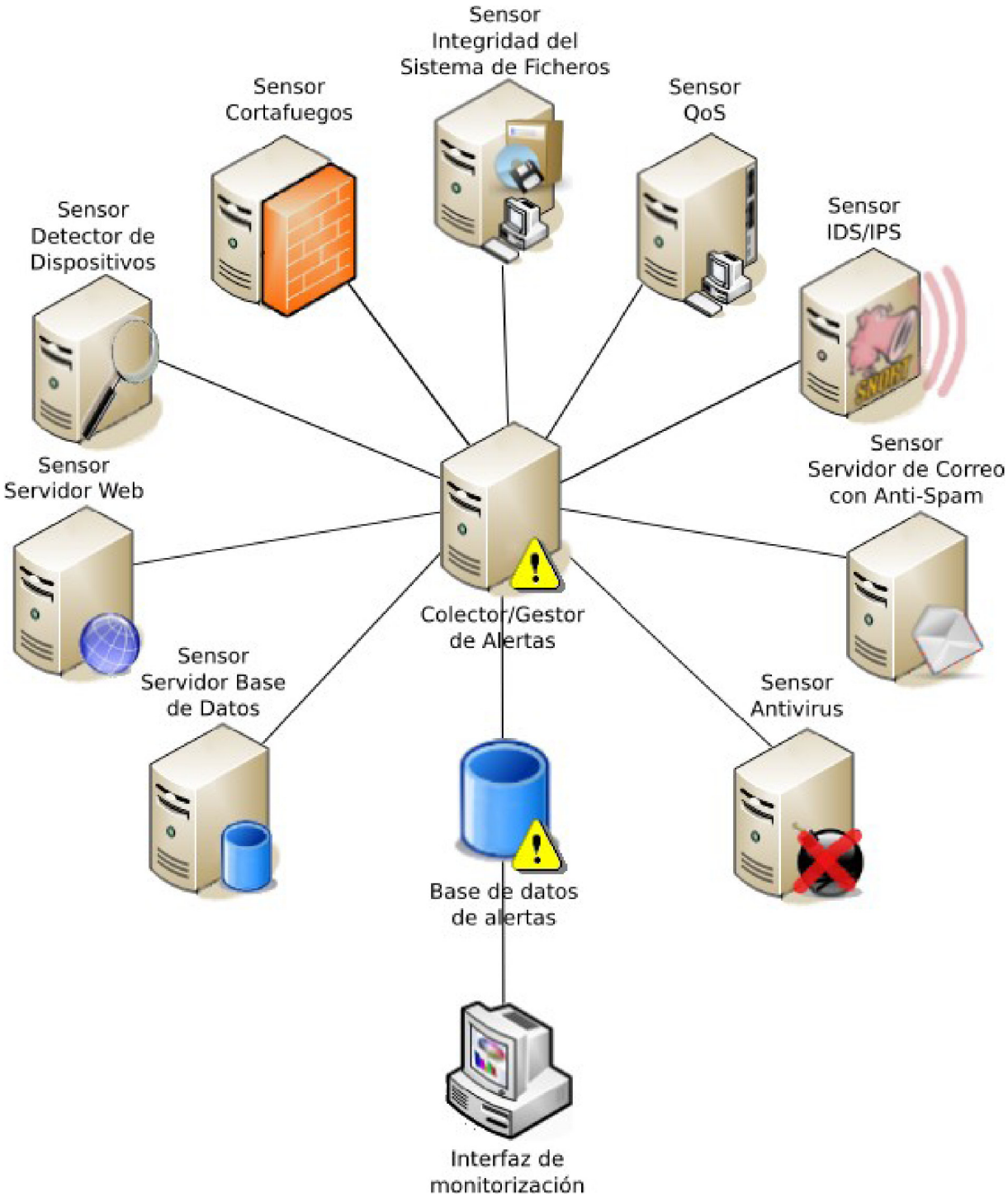

Figura 1: Escenario del sistema de monitorización y gestión de mensajes.

En nuestro escenario dispondremos de una serie de sensores, entendiendo por sensor todo dispositivo capaz de generar mensajes que pueda recopilar el colector/gestor de logs.

A modo de ejemplo, los sensores de cortafuegos emitirán mensajes o alertas cuando detecten un intento de conexión por un puerto cerrado.

El detector de dispositivos cuando se conecte una nueva máquina a la red local.

Un servidor web puede ser un sensor si se redireccionan al colector los mensajes del fichero */var/log/apache.log* o equivalente, almacenando por ejemplo al autenticarse en páginas PHP ó ASP alojadas en dicho servidor.

Los servidores de base de datos podrían configurarse para generar una alerta ante una transacción incompleta, base de datos al 80% de la capacidad....etc.

El sensor antivirus informará de nuevos virus o caballos de Troya detectados en el sistema.

El servidor de correo electrónico, si dispone de filtro anti-Spam, informará de correo no deseado reincidente, desbordamiento por correo deseado, cuota de almacenamiento sobrepasada para un usuario, etc.

El sistema de detección de intrusiónes IDS o el de prevención de intrusiones IPS será el principal informador de alertas, ya que se le podrán definir cantidad de reglas para emitir mensajes al detectar mensajes ICMP ping, escaneo de puertos, envío de paquetes sin encriptar, etc.

El sensor de calidad del servicio o QoS emitirá cuando una aplicación o usuario sobrepase la fracción de ancho de banda asignado, siempre que se disponga de software para el control de este parámetro.

En la instalación de un virus, caballo de Troya o agente informático perjudicial en general, se puede corromper el sistema de ficheros o atentar contra la integridad de los ficheros del sistema. Esto es especialmente crítico en servidores de ficheros con datos confidenciales. Un sensor instalado en un sistema de estas características informa de cualquier cambio en los ficheros de sistema.

El colector/gestor de logs es capaz de recopilarlos, procesarlos y almacenarlos en una base de datos lo suficientemente compleja y versátil como para albergar toda la información de los mensajes de distinta categoría. Uno de los principales problemas será la inhomogeneidad del formato de dichos mensajes, ya que, aunque posean campos comunes, el orden en el que se empaquetan es diferente así como la aparición o no de otros campos del mensaje. De la unificación del formato se podrían encargar los sensores (Habría que disponer de un plugin para ello), el gestor de alertas (Tendría que adaptarse a todos los formatos diferentes de los sensores, lo cual es muy complejo) u otro dispositivo intermedio que hiciese la traducción a un formato único que comprendiese el gestor para almacenarlo en la base de datos de forma homogénea.

Por último, la interfaz de monitorización se encargará de procesar, agrupar los datos mediante consultas a la base de datos para presentar estadísticas al administrador de red del tipo: Lista de orígenes que han generado más alertas, destinos, protocolos, puertos, tipo de mensaje, intervalos más críticos etc, ordenándolos por fecha, por dirección IP y un sin fin de posibilidades configurables por el administrador de red.